(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 899 647 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
03.03.1999 Bulletin 1999/09

(51) Int Cl.[6]: **G06F 1/00**

(21) Application number: **98306651.5**

(22) Date of filing: **19.08.1998**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.08.1997 US 927096**

(71) Applicant: **Compaq Computer Corporation**
Houston Texas 77070 (US)

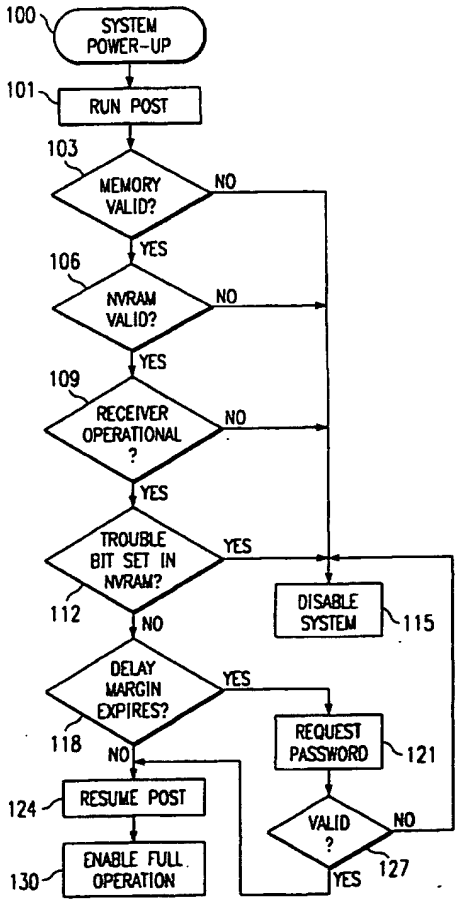
(72) Inventors:
- **Angelo, Michael F.**
Houston, Texas 77068 (US)
- **Olarig, Sompong P.**
Cypress, Texas 77429 (US)

(74) Representative: **Brunner, Michael John**
GILL JENNINGS & EVERY
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(54) Remote security technology

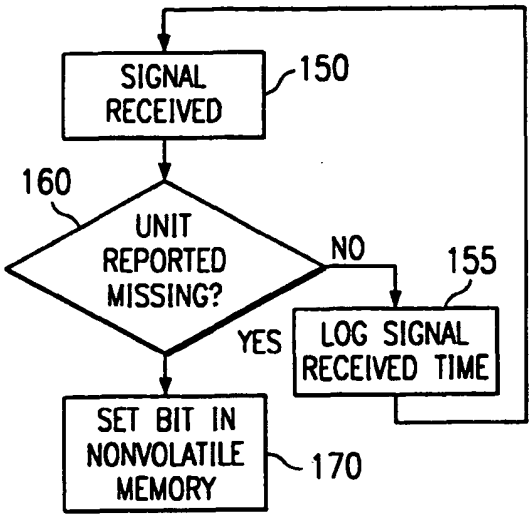
(57) A computer (or other complex electronic equipment) security system is proposed whereby access is controlled by remote enablement or disablement of a security feature. The system can be coupled with third-party products to accommodate satellite transmissions for long-distance access control.

FIG. 1A



EP 0 899 647 A2

FIG. 1B



Description

[0001] This invention relates to a method for computer security whereby commands can be sent remotely to the computer such that operation is enabled or disabled. Physical computer equipment, and intellectual property stored on hard drives in portable computers, can be worth millions of dollars to the owner companies. Particularly where small, expensive, and portable computers are involved, asset management is becoming very difficult.

[0002] With the advent of the Internet and pervasiveness of computers in business and personal life, it is only natural that theft of such equipment, components, and information stored on these systems becomes more prevalent. Employees continue to be the primary source for losses due to theft. For example, employees who have compatible systems at home may be tempted to swap boards and input devices at work to repair their systems at home. Employees are not the only threat. Repairmen, janitors, delivery-persons, other contractors, customers, invited guests, and even security people themselves have an opportunity to take computer property.

[0003] Size and portability are also factors. As integrated circuit manufacturers reduce the size of chips with a complementary boost in performance and power, the boxes into which the chips are placed become smaller. Grab-and-run thefts are likely to focus on the smallest equipment. As computer equipment continues to decrease in size (e.g. sub-notebook and smaller computers), the chance of losing it to theft increases. The reduction in size certainly seems to be the way of the future.

[0004] Intellectual property comprises a significant part of company's asset portfolio. In many cases, the value of a piece of intellectual property far exceeds the value of the hardware on which is stored. Consequently, if the hardware is stolen, the ability to prevent access to that information is paramount, and return of the hardware is only a secondary objective. A survey of 325 U. S. companies by the American Society for Industrial Security concluded that potential losses to U.S. companies could total $24 billion a year.

[0005] Computers and related peripherals, and intellectual property are not the only target of high-tech theft. State-of-the-art instrumentation and test equipment are also prime candidates and are usually more expensive per unit volume than a typical home computer. Although less marketable than computer equipment, they can represent a sizeable loss to companies using such equipment.

[0006] Companies are becoming increasingly concerned about the loss or illicit disclosure of corporate proprietary information. Protection of stored information is accomplished primarily by hard disk software security locks and data encryption. These measures are not absolutely theft-proof and in many cases can be defeated rather easily. Furthermore, once defeated, the system is useable. For example, theft of a laptop with a software protected hard disk can be defeated by simply swapping in a new or different compatible drive without the software protection a small price to pay relative to the value of the whole system. Moreover, removal of the laptop computer to a different location will in many cases provide ample time to defeat the software locks and encryption employed to secure the information.

[0007] However, in some cases, the theft is for the value of the hardware and not the information contained on the system storage devices. Thus, most hardware security systems attempt to protect the computer system by fixing it to another less mobile object. However, once a security cable is removed, the computer is still fully operational and easily resalable.

[0008] These prior art measures are ineffective where the computer equipment has yet to be secured, for example, during shipment to the consumer or during assembly at the manufacturer. Furthermore, the conventional methods are ineffective against theft from a car or from the person. As mentioned before, as integrated circuits become smaller, the more functions that can be designed into a chip and the more densely populated a board becomes. Eventually, all electronic functions of the computer may be integrated into one board. Conventional theft protection methods do not provide the level of protection in these situations to discourage theft of a board or system.

[0009] One difficulty in preventing this problem is that most users are unwilling to go to the inconvenience of using passwords or other security measures. Therefore, although some of today's systems have POST passwords or encryption devices built in, very few of these features are actually enabled, and therefore it is difficult for companies to ensure that systems are secure. Currently, if such a system is lost or stolen while its security features are disabled, there is no way for the owner to prevent its unauthorized use.

[0010] The automotive industry has made some use of remotely-activated anti-theft devices. A popular system is called LoJack and is used to track stolen vehicles. To protect a car, a transmitter/receiver unit is attached in an inconspicuous place. If the car is stolen, the owner notifies the police. The police then remotely activate the transmitter, which sends a continuous signal allowing police to locate and recover the car. The disadvantage with this system is that the owner must first discover, and notify authorities, that the property has been stolen. Thus it is possible for the thieves to drive the vehicle away when the owner is not aware of the theft, and work for several hours at defeating the anti-theft device or stripping the car. Furthermore, a seasoned thief can easily disable or even remove the transmitter/receiver device, thereby defeating the effectiveness of this anti-theft system.

[0011] Other products use Global Positioning System ("GPS") satellites to let distressed drivers call for help

or authorities to track stolen cars. The driver must connect a cellular phone installed in the vehicle and enter a pass-code when starting the car.

[0012] Further disadvantages of these and related systems are that the owner pays monthly service charges for use of the system. In other designs, it requires that the system be active, and plugged into a phone system. Up-front costs are high for parts and installation. In addition, many solutions reduce the ability to perform work and are subsequently not used.

[0013] In general, any remotely activated anti-theft add-on which is inoperative when the system is inoperative has a serious weakness: if the system can be physically removed while inoperative, a thief can take it to a shielded location and work at length on disassembling the system or removing the protection.

[0014] According to the present invention there is provided a complex electronic system, comprising: at least one microprocessor operatively connected to detect inputs from an input device; a nonvolatile memory containing settings for administrative configurations; a memory which is connected to be read/write accessible by said microprocessor; input/output circuitry operatively connected to said microprocessor; and an RF receiver operatively connected to write to said nonvolatile memory, said receiver being receptive to a communication system; wherein said system includes at least one security feature which can be remotely activated by commanding said receiver, through said communication system, to modify at least one of said settings in said nonvolatile memory.

[0015] The invention also includes a system security method, comprising the steps of: (a) receiving a security-activation command from an RF transmitting source; and (b) selectively changing at least one administrative configuration options of a system to activate at least one security feature, based upon said command.

[0016] The present invention thus incorporates a new type of security feature into the circuitry of a portable computer (or analogous equipment). The computer contains an RF receiver unit which is always active, even when the computer is not. If the computer is reported stolen, a signal is sent to the receiver to activate a security feature (such as boot password protection), even if the user had previously inactivated this security feature. When the computer is next turned on, this security feature will prevent the thief from making use of the computer.

[0017] This security architecture, in the presently preferred embodiment, does not permanently destroy operation of the system, but simply restores the system's built-in security protection options. This is done by setting a bit in nonvolatile memory, which thereafter makes the system require a password for access to operate the system. (If the user has not enabled password protection, he will have to get an emergency password from his system administrator or from technical support.) An important feature of this embodiment is that it is executed during the system Power-On Self-Test ("POST") procedure, and thus cannot be bypassed.

[0018] An advantage is that the feature can be coupled to existing third-party communication systems to allow a command to be received by the computer in order to disable operation to unauthorized owners. For example, Eagle Eye Technologies, Inc., builds a tracking system that is capable of locating a transponder to within 3 meters of its actual location. The present application uses a slightly different technique, based upon the same radio frequency (RF) interfacing hardware, to set an electronic key bit in non-volatile RAM of a computer (or a comparably complex mobile or portable unit) which impedes operation of the unit if a security command is sent. Thieves will be reluctant to steal a device with this feature.

[0019] Another advantage is obtained at a lower level. With the feature integrated onto the system board, the board itself can be disabled from operating. This prevents board swapping by employees to home computers.

[0020] Another advantage is the protection of user data at a higher level. Theft of proprietary information is more difficult in that one more barrier is added to the process. If the system is disabled, the thief must remove the storage unit and install it into a compatible system in order to steal the information.

[0021] Another advantage over prior art security systems is that systems are secure during shipment and while sitting in a warehouse. If a shipment disappears, its illegitimate operation can be disabled from any point in the country, or perhaps even the world.

[0022] Preferably the satellite receiver is always on, and thus can be commanded to set the security feature even if the system is powered down. This prevents thieves from taking a stolen computer into a shielded room to defeat its protection.

[0023] Another advantage is that the system can be secured after it has been lost or stolen, even if the original user did not take advantage of conventional security features.

[0024] While activation of a boot password requirement is the preferred security feature, in alternative embodiments other security features can be activated instead. For example, one simple (but less preferred) choice is simply to lock down the system unconditionally. This is less preferred, since it is more likely to cause serious inconvenience to a legitimate user if erroneously activated.

[0025] In another embodiment, rather than marking a bit in non-volatile memory, the system can permanently activate the security feature by blowing a fuse in a key circuit.

[0026] In another embodiment, rather than marking a bit in non-volatile memory, the system can alternatively disable the hardware by blowing a fuse in a key circuit.)

[0027] In another embodiment, rather than marking a bit in non-volatile memory, the system can alternatively

set a bit in CMOS. However, this alternative is less preferred, since CMOS settings can be cleared by physically removing the CMOS backup battery.

[0028] In yet another embodiment, the security feature can be checked at other times as well, e.g. when a plug-and-play update occurs, or whenever a wakeup from sleep mode occurs.

[0029] In other embodiments, other security features can be used instead of or in addition to the boot passwording and/or lockdown features stated above.

[0030] Instead of noting the time a signal was received, the system can use a timer to determine if a valid signal was received within the allotted time period.

[0031] The preferred embodiment utilizes a system in which a periodic signal is sent to the unit to ensure that communications are still possible. Alternatively, the POST program can initiates a request for a status check, then wait for a response.

[0032] The disclosed security system can be used in concert with other third-party communications products, such as global tracking systems to locate the system after theft.

[0033] Sample embodiments of the invention will now be described with reference to the accompanying drawings in which:

Figure 1A shows a flowchart of the security control process.

Figure 1B shows a flowchart of the security control process of the receiver system.

Figure 1C shows a flowchart of the overall security control process once a device is determined stolen from the owner.

Figure 2 shows a portable computer block diagram which can use the innovative remote security architecture.

[0034] With reference to the flowchart of Figure IC, upon first notification from the owner that a device with the innovative embodiment has been stolen, the entity responsible for activating the security mechanism receives the stolen-property report and initiates the security process (step 180). Next, a verification process executes to ensure that owner is correctly identified with the appropriate piece of equipment (step 182). When the verification process is completed, the necessary commands are uploaded to a worldwide positioning system (step 184) for satellite broadcast to the device (step 186). A "locate and lock" sequence is executed (step 188) resulting in the device being disabled by the respective locking circuitry. In this case, a chip made by M2M, sets a bit in NVRAM (step 190) triggering the security querying process set forth below.

[0035] Figure 1B shows a flowchart of action of the receiver portion of the security control process. This portion of the process is initiated by the reception of a signal (step 150). Whenever a signal is received by the security system, the signal is evaluated (step 160) to determine if that specific unit has been reported missing, and should therefore be locked. As long as the signal indicates that the unit is not missing, the security system will log a time that the last signal was received (step 155), then return to wait for the next signal. When the signal indicates that the unit has been reported missing, the system will set a bit in non-volatile memory to indicate that the unit should be disabled (step 170).

[0036] Note that the receiver circuit is always active, even when the system itself is turned off. Since this is the case, the disable signal can be sent at any time, and the system will be secured. As described below, the user may not be aware that the system is disabled until the next use.

[0037] Figure 1A shows a flowchart of the security control process when the computer is activated. First, the user turns power on to the system (step 100). Shortly thereafter, the computer POST (step 101) procedure begins to execute. The system performs a memory test (step 103) and NVRAM test (step 106). If any of the memory checks fail, the system will be disabled (step 115). If the memory checks okay, the process continues with hardware checks of the receiver circuitry (step 109). If the trouble bit was set in NVRAM (step 112) either from a prior disabling command or by attempts to deactivate the circuitry, system operation remains disabled (step 115). If the receiver checks okay (step 109), the next step is to determine if a command has been received setting the trouble bit in NVRAM (step 112), disabling the system (step 115). If yes, the system is disabled (step 115). If not, the system verifies that a periodic enabling signal has been received within the required time delay margin (step 118), by comparing the time the last signal was received with the internal clock. If yes, the POST (step 124) procedure resumes and upon successful completion, enables full system operation (step 130). If the delay margin has expired (step 118), the system makes one more attempt to obtain the required password (step 121) and keep the system operational. If the password is invalid (step 127), the system is disabled (step 115). If the password is valid (step 127), the system remains fully operational (step 130). The authorization scheme is such that a denial-of-service situation is employed only in extreme cases.

[0038] Figure 2 shows a portable computer which can use the innovative remote security architecture. The system includes a power converter 205 which is used to charge a battery 215. Optionally, a battery interface 210 is interposed between the battery and the rest of the circuitry. The power converter 205 is connected, through a full-wave bridge rectifier 200 to draw power from AC mains, and is connected to provide a DC voltage to the battery 215. The battery 215 (or the converter 205), connected through a voltage regulator 220, is able to power the complete portable computer system, which includes in this example:

user input devices *(e.g.* keyboard 235 and mouse

240);
at least one microprocessor 225 which is operatively connected to receive inputs from said input device, through an interface manager chip 230 (which also provides an interface to the various ports);
a memory *(e.g.* flash memory 255 and RAM 260), which is accessible by the microprocessor;
a data output device *(e.g.* display 250 and video display adapter card 245) which is connected to output data generated by microprocessor;
a magnetic disk drive 270 which is read-write accessible, through an interface unit 265, by the microprocessor; and
an electronic options circuit 295 for receiving current location information from a worldwide positioning system and selectively enabling or disabling operation of the computer system.

[0039] Optionally, of course, many other components can be included, and this configuration is not definitive by any means. For example, the portable computer may also include a CD-ROM drive 280 and floppy disk drive ("FDD") 270 which may interface to the disk interface controller 265. Additionally, L2 cache 285 may be added to speed data access from the disk drives to the microprocessor, and a PCMCIA 290 slot accommodates peripheral enhancements.

[0040] In a further example, use of the invention in motor vehicles allows authorities to disable operation of the vehicle upon notification of its theft, or for any other reason deemed necessary.

[0041] Another use of the invention in expensive cellular telephones will provide a deterrent to theft. The ability to disable device operation when stolen from its rightful owner has a substantial impact on its value to a thief.

[0042] Asset management is often a problem in large companies. In a further class of embodiments, if a particular piece of equipment (e.g. a portable computer) cannot be found at inventory, the disclosed security system can be used to simply disable it. If the equipment has been legitimately transferred, the legitimate user will then be forced to call in for service, and the equipment can then be reactivated. (Of course appropriate precautions would be necessary before such a procedure could be applied to equipment which might cause harm by suddenly going out of service.)

[0043] Implementations of the invention feature into high-tech instrumentation will prohibit theft of this very costly type of equipment. Such components may include one or more programmable processors, and may have a system reset procedure into which the described security relations can be inserted.

[0044] As will be recognized by those skilled in the art, the innovative concepts described in the present application can be modified and varied over a tremendous range of applications, and accordingly the scope of patented subject matter is not limited by any of the specific exemplary teachings given.

Claims

1. A complex electronic system, comprising:

   at least one microprocessor operatively connected to detect inputs from an input device;
   a non-volatile memory containing settings for administrative configurations;
   a memory which is connected to be read/write accessible by said microprocessor;
   input/output circuitry operatively connected to said microprocessor; and
   an RF receiver operatively connected to write to said non-volatile memory, said receiver being receptive to a communication system;

   wherein said system includes at least one security feature which can be remotely activated by commanding said receiver, through said communication system, to modify at least one of said settings in said non-volatile memory.

2. The system of Claim 1, wherein said receiver is integral with said system.

3. The system of Claim 1 or Claim 2, wherein said security feature is a boot password requirement.

4. The system of any of the preceding claims, wherein said system will not function without said receiver.

5. The system of any of the preceding claims, wherein said receiver is a wireless device.

6. The system of any of the preceding claims, wherein said communications system uses radio frequency.

7. The system of any of the preceding claims, wherein said receiver is integrated into a system board which also carries said microprocessor.

8. The system of any of the preceding claims, wherein said receiver is active even when said microprocessor is asleep.

9. The system of any of the preceding claims, wherein said receiver is also operatively connected to selectively force said microprocessor into a reset procedure.

10. The system of any of the preceding claims, wherein the decision to enable or disable operations is included with a Power-On Self-Test procedure.

11. The system of any of the preceding claims, wherein

operation of said system is automatically disabled if an electronic key bit is set in memory.

12. The system of any of the preceding claims, wherein operation of said system is automatically disabled if said receiver is not operational.

13. The system of any of the preceding claims, wherein operation of said system is disabled if a valid password is not entered when requested.

14. The system of any of the preceding claims, comprising a computer system.

15. The system of any of claims 1 to 13, comprising a motor vehicle.

16. The system of any of claims 1 to 13, comprising a cellular telephone.

17. A system security method, comprising the steps of:

(a) receiving a security-activation command from an RF transmitting source; and
(b) selectively changing at least one administrative configuration options of a system to activate at least one security feature, based upon said command.

18. The method of Claim 17, wherein said step (b) also forces the system into a reset operation.

19. The method of Claim 17 or Claim 18, wherein said receiving step uses a receiver which is constantly active, even when other portions of the system are inactive.

20. The method of any of claims 17 to 19, wherein said security feature is conditionally activated during an automatic Power-On Self-Test procedure of said computer.

21. The method of any of claims 17 to 19, wherein said security feature is boot password protection.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 899 647 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
23.02.2000 Bulletin 2000/08

(43) Date of publication A2:
03.03.1999 Bulletin 1999/09

(21) Application number: **98306651.5**

(22) Date of filing: **19.08.1998**

(51) Int Cl.[7]: **G06F 1/00**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.08.1997 US 927096**

(71) Applicant: **Compaq Computer Corporation**
Houston Texas 77070 (US)

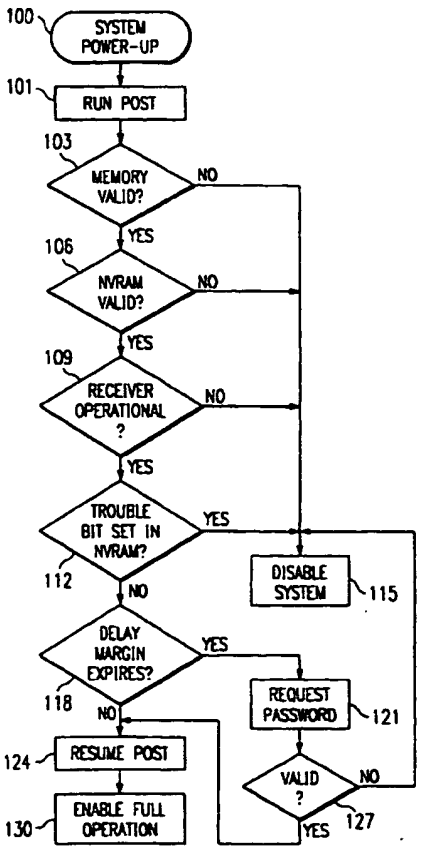
(72) Inventors:
- **Angelo, Michael F.**
  Houston, Texas 77068 (US)
- **Olarig, Sompong P.**
  Cypress, Texas 77429 (US)

(74) Representative: **Brunner, Michael John**
GILL JENNINGS & EVERY
Broadgate House
7 Eldon Street
London EC2M 7LH (GB)

(54) Remote security technology

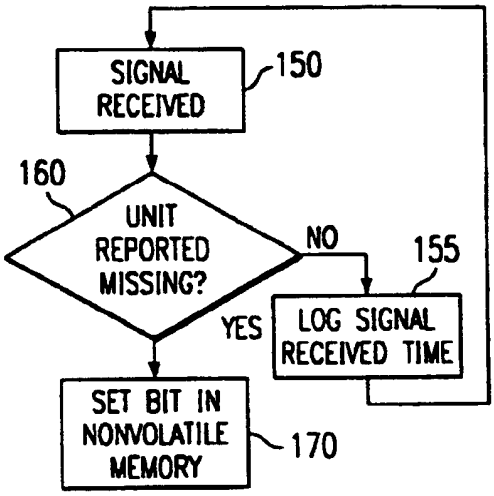
(57) A computer (or other complex electronic equipment) security system is proposed whereby access is controlled by remote enablement or disablement of a security feature. The system can be coupled with third-party products to accommodate satellite transmissions for long-distance access control.

FIG. 1A



EP 0 899 647 A3

FIG. 1B



European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 98 30 6651

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	US 5 046 082 A (BLAIR KEVIN B ET AL) 3 September 1991 (1991-09-03) * column 1, line 17 - line 35 * * column 3, line 16 - column 4, line 59 *	1,2,4-8, 12, 15-17,19	G06F1/00
Y		3,9,10, 13,14, 18,20-22	
P,X	US 5 748 084 A (ISIKOFF JEREMY M) 5 May 1998 (1998-05-05) * abstract; figures 3,4 * * column 1, line 48 - column 4, line 61 *	1,2,4-7, 12,14, 16-18	
P,X	EP 0 836 131 A (HEWLETT PACKARD CO) 15 April 1998 (1998-04-15) * column 1, line 1 - column 5, line 23 *	1,2,5,6, 14,17	
Y	EP 0 449 242 A (NAT SEMICONDUCTOR CORP) 2 October 1991 (1991-10-02) * abstract; figures 2,4 * * page 3, line 43 - page 4, line 46 * * page 11, line 52 - page 12, line 1 *	3,9,10, 13,14, 18,20-22	TECHNICAL FIELDS SEARCHED (Int.Cl.6) G06F
A	US 5 418 537 A (BIRD DAVID G) 23 May 1995 (1995-05-23) * abstract; figure 4 *	8,15,19	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	21 December 1999	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 98 30 6651

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

21-12-1999

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5046082 A	03-09-1991	NONE	
US 5748084 A	05-05-1998	NONE	
EP 0836131 A	15-04-1998	JP 10124345 A	15-05-1998
EP 0449242 A	02-10-1991	US 5475839 A	12-12-1995
US 5418537 A	23-05-1995	US 5777580 A	07-07-1998